



Institute for Scientific Computing Research



Annual Report

Fiscal Year

2003



The University Relations Program (URP) encourages collaborative research between Lawrence Livermore National Laboratory (LLNL) and the University of California campuses. The Institute for Scientific Computing Research (ISCR) actively participates in such collaborative research, and this report details the Fiscal Year 2003 projects jointly served by URP and ISCR. For a full discussion of all URP projects in FY 2003, please request a copy of the URP FY 2003 Annual Report by contacting

Lawrence Livermore National Laboratory
Edie Rock, University Relations Program
P. O. Box 808, L-413
Livermore, CA 94551

UCRL-TR-202404



DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from the Office of Scientific and Technical Information
P.O. Box 62, Oak Ridge, TN 37831
Prices available from (423) 576-8401

Available to the public from the National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Rd., Springfield, VA 22161

ISCR Fiscal Year 2003 Director's Report.....	4
Institute for Terascale Simulation Lectures	11
Quantum Computation and Information Seminars	17
ISCR Seminar Series.....	33
ISCR Summer Student Program.....	79
ISCR Sabbatical Program.....	149
University Collaborative Research Program.....	161
Laboratory Directed Research and Development (LDRD) Projects.....	181
ISCR Research Subcontracts.....	189
Workshops and Conferences	219

The Mission of the ISCR

The Institute for Scientific Computing Research (ISCR) at Lawrence Livermore National Laboratory (LLNL) identifies collaborators from the academic community for computer science and computational science research and development efforts at the Laboratory and hosts them in short- and long-term residential visits, with the aim of encouraging long-term academic research agendas that address Laboratory research priorities. Through such collaborations, ideas and software flow in both directions, and the Laboratory cultivates its future workforce. An extensively externally networked ISCR cost-effectively expands the level and scope of computational science expertise available to the Laboratory. As large-scale simulations on the parallel platforms of DOE's Advanced Simulation and Computing program (ASCI) and other terascale platforms become increasingly important to the overall mission of LLNL, the role of the ISCR expands in importance, accordingly.

The ISCR forms academic partnerships with the University of California (UC), with universities throughout the United States, and internationally. The primary consideration is to identify the highest quality, most topically opportune, and potentially most vigorous partnerships. The special relationship between LLNL and the University of California and the geographical proximity

of UC's campuses tend to make collaborations with UC faculty and students particularly effective.

The ISCR strives to be the "eyes and ears" of the Laboratory in the computer and information sciences, keeping the Laboratory aware of and connected to important external advances. It also attempts to be "feet and hands" in carrying those advances into the Laboratory and incorporating them into practice. In addition to conducting research, the ISCR provides continuing educational opportunities to Laboratory personnel in the form of on-site workshops taught by experts on novel software or hardware technologies.

Through the workshops, visits, and internships it sponsors, ISCR also seeks to influence the research community external to the Laboratory to pursue Laboratory-related interests and to train the workforce that will be required by the Laboratory, because some of its needs are not otherwise well reflected in university curricula or the commercial information technology environment. Part of the performance of this function is interpreting to the external community appropriate (unclassified) aspects of the Laboratory's own contributions to the computer and information sciences, contributions that its unique mission and unique resources give it a unique opportunity and responsibility to make.

Institute for Scientific Computing Research

Fiscal Year 2003 Director's Report

Large-scale scientific computation and all of the disciplines that support it and help to validate it have been placed at the focus of Lawrence Livermore National Laboratory by the Advanced Simulation and Computing (ASCI) program of the National Nuclear Security Administration and the Scientific Discovery through Advanced Computing (SciDAC) initiative of the Office of Science of the Department of Energy (DOE). The Laboratory operates computers with among the highest peaks of performance in the world and has undertaken some of the largest and most compute-intensive simulations ever performed. Secretary of Energy Spencer Abraham announced in November 2003 that ultrascale simulation is one of the highest priorities in the DOE's facilities planning for the next two decades. However, computers at architectural extremes are notoriously difficult to use efficiently. Furthermore, each successful terascale simulation only points out the need for much better ways of interacting with the resulting avalanche of data.

Advances in scientific computing research have therefore never been more vital to the core missions of the Laboratory than at present. Computational science is evolving so rapidly along every one of its research fronts that to remain on the leading edge the Laboratory must engage researchers at many academic centers of excellence. In FY 2003, the Institute for Scientific Computing Research (ISCR) served as one of the Laboratory's main bridges to the academic community in the form of collaborative subcontracts, visiting faculty, student internships, workshops, and an active seminar series.

ISCR research participants are integrated into the Laboratory's Computing and Applied Research (CAR) Department, especially into its Center for Applied Scientific Computing (CASC). These organizations, in turn, address computational challenges arising throughout the rest of the Laboratory. Administratively, the ISCR flourishes under the Laboratory's University Relations Program (URP). Together with the other institutes of the URP, it navigates a course that allows the Laboratory to benefit from academic exchanges while preserving national security. While it is difficult to operate an academic-like research enterprise within the context of a national security laboratory, the results declare the challenges well met and worth the continued effort.

Fiscal year 2003 was the fourth full year under Acting Director David Keyes. Keyes, the Fu Foundation Professor of Applied Mathematic at Columbia University and an ISCR faculty participant since October 1997, dedicated one-third of his time to the technical program of the ISCR. Dr. James McGraw continued as the Deputy Director of the ISCR, while also serving in a special national role last year as the General Chair of the record-breaking SC 2003 conference. Linda Becker continued as the full-time Institute Administrator. Emma Horcabas and Leslie Bills logistically supported the large visitor and summer programs of the ISCR. They were assisted by Pam Mears, who joined the ISCR full-time.

The ISCR continues to have a small contingent of research staff members within its organization. Three ISCR staff—Prof. Nelson Max, Prof. Garry Rodrigue, and Prof. Rao Vemuri—hold joint appointments as professors at UC Davis and senior researchers at LLNL. In addition, the ISCR hosted eight post-doctoral staff: Alison Baker, David Buttler, Samson Cheung, Shawn Newsam, Dan Reynolds, Markus Schordan, Megan Thomas, and Qing Yi. Finally, the ISCR served as the host for ten students (listed in Table 1) who attend the University of California, Davis on a Student-Employee Graduate Fellowship. This fellowship enables students to work with LLNL researchers half-time while pursuing their PhDs.

The ISCR enables substantial interactions between academia and LLNL staff through consultants and participating guests. Consulting agreements are vehicles for permitting academics to interact with LLNL in a compensated fashion. Consultants can serve on special review committees, present classes on specific focus topics, and/or visit LLNL periodically for technical meetings. All consultants have a specific LLNL technical point of contact for overseeing the interactions. Table 2 lists the ISCR consultants for FY 2003. Participating Guests are researchers from academia or industry that often need intermittent access to LLNL staff (and resources), where funding is not the critical issue. This status permits an appropriate security clearance and the ability to quickly arrange for on-site visits with LLNL staff over a period of one month to two years. Table 3 lists ISCR's participating guests for FY 2003.

The pages of this report summarize the activities of the faculty members, post-doctoral researchers, students, and guests from industry and other laboratories who participated in LLNL's computational mission under the auspices of the ISCR during FY 2003. These activities fall under two main themes: sponsored research activities that stimulate interactions between academia and LLNL staff, and a diverse visitor program that enables both short- and long-term residential stays at LLNL.

ISCR oversees three different types of sponsored-research activities. The University Collaborative Research Program (UCRP), through the ISCR, funds typically six to nine research

Student	LLNL Advisor	Term at LLNL
Peer-timo Bremer	Dan Laney	6/02-6/06
Sam Brockington	Garry Rodrigue, Dave Hwang	10/01-8/06
Aaron Fisher	Garry Rodrigue	7/02-6/06
Benjamin Gregorski	Mark Duchaineau	6/01-6/05
Jeff Hagelberg	Paul Amala	9/03-9/04
Aaron Herrnstein	Michael Wickett	3/01-3/04
Ana Iontcheva	Panayot Vassilevski	9/00-8/03
Rob Rieben	Garry Rodrigue	10/00-9/04
Joshua Senecal	Mark Duchaineau	11/01-10/05
Yihao Zheng	Andy Wissink	7/02-8/03

Table 1: FY 2003 ISCR Student Employee Graduate Research Fellowships

projects each year at campuses of the University of California. These projects primarily support graduate students working on thesis research that focuses on a topic of interest to LLNL. The faculty principal investigators and students are expected to work closely with an LLNL collaborator. The ISCR also coordinates the funding of numerous research subcontracts to various academic institutions throughout the United States. These contracts are normally funded by programs at LLNL with the express intent of helping to address long-term Laboratory research interests. In many cases, this type of vehicle is used to fund sabbatical visits to LLNL for three to six months. With Laboratory Directed Research and Development (LDRD) funds, the ISCR also funds Exploratory Research in the Institutes (ERI). These research grants go to LLNL staff with the goal of developing ties to academia through co-funded research projects. Annual progress reports for UCRP-funded projects, subcontracts, and ERI projects can be found in the next three sections of this document.

In FY 2003 the ISCR continued its tradition of an extensive and diverse Visitor Program. This program includes sabbatical visitors, sponsored workshops, summer students, and three different seminar series featuring external speakers. The ASCI Institute

Consultant	Affiliation	LLNL Contact
Randolph Bank	UC San Diego	Charles Tong
Leo Breiman	UC Berkeley	Chandrika Kamath, Imola Fodor
Gene Golub	Stanford University	Edmond Chow
Anne Greenbaum	University of Washington	Peter Brown
Charles Hansen	University of Utah	Randy Frank
Heinz-Otto Kreiss	UC Los Angeles	David Brown
Thomas Manteuffel	University of Colorado, Boulder	Rob Falgout
Stephen McCormick	University of Colorado, Boulder	Rob Falgout
Linda Petzold	UC Santa Barbara	Peter Brown
Sandu Popescu	Bristol University	Patrice Turchi
Steve Schaffer	New Mexico Inst. of Mining and Technology	Rob Falgout, Jim Jones
Homer Walker	Worcester Polytechnic Institute	Carol Woodward

Table 2: FY 2003 ISCR Consultants

for Terascale Simulation Lecture Series was established to enrich the intellectual atmosphere of LLNL's large simulation community through the visits of leaders throughout the diverse areas of computation. In FY 2003 we hosted three speakers in this series. ISCR also co-hosted (with the Materials Research Institute) a special topical series on Quantum Computing that included 14 of the most prominent researchers in this emerging field. The general ISCR seminar series included an additional 43 talks covering a wide spectrum on research areas. Abstracts on all of these talks can be found in the Seminar Series section of this report.

Guest Name	Institution		
Marian Brezina	University of Colorado, Denver	Sally McKee	Cornell University
Alok Choudhary	Northwestern University	Michael Minion	University of North Carolina
Hans de Sterck	University of Colorado, Boulder	R. Frank Mueller	North Carolina State University
Branden E. Fitelson	UC Berkeley	Esmond Ng	Lawrence Berkeley Laboratory
Franz Franchetti	Technical University of Vienna	Beth Ong	LLNL (on leave)
Alejandro Garcia	San Jose State University	Peter Pacheco	University of San Francisco
Matthew R. Gibbons	U.S. Air Force Academy	Joseph Pasciak	Texas A&M University
Michael Griebel	University of Bonn	Joanne Perra	LLNL retired
Bernd Hamann	UC Davis	Christoph Pflaum	University of Erlangen
Alan Hindmarsh	LLNL (retired)	Elbridge Gerry Puckett	UC Davis
Ken Joy	UC Davis	Markus Pueschel	Carnegie Mellon University
Andrew Knyazev	University of Colorado, Denver	Ulrich Ruede	University of Erlangen
Johannes Kraus	University of Loeben	Paul Saylor	University of Illinois
Raytcho Lazarov	Texas A&M University	Martin Schultz	Cornell University
Lars Linsen	UC Davis	Claudio Silva	Oregon Graduate Institute
Oren Livne	Stanford University	Christoph W. Ueberhuber	Vienna University of Technology
Bertram Ludaescher	San Diego Supercomputer Center	Beata Winnicka	Argonne National Laboratory
Jennifer Mariani	UC Davis	Ludmil Zikatanov	Penn State University

Table 3: FY 2003 ISCR Participating Guests

Twenty-four faculty visitors were in residence for more than just a seminar visit—visits ranged from a week to a semester. Six of these faculty spent a portion of their sabbatical leave here. Altogether, the ISCR hosted 162 visits from 125 different visitors, an average of more than three visits per week. The vast majority of the visitors were from academia, with 17% from industry and 10% from other laboratories. Visitors from outside the United States made up 31% of the total.

During the summer, ISCR hosted 63 visiting students. The summer program exposes students to the stimulating and challenging work environment of a national laboratory. Successful candidates are hired as summer employees, assigned individual LLNL mentors, and given specific projects to which they will contribute. The nature of the project and contribution are determined so as to complement their background and skills. The topical coverage of the summer research program broadens each year as computation expands into new scientific areas and as computational tools become more powerful and diverse. Optimal algorithms, fluid turbulence, genomics, terascale visualization, and computer security are just a handful of topics from the lively summer hallway conversation at the ISCR! The summer program runs from mid-May to late September, with most participants spending 10–12 weeks on site. Project reports for most of the students can be found later in this report.

In June, with the advent of our large student summer program and sponsorship from the Defense Programs office of DOE Headquarters, we ramped up our fourth annual

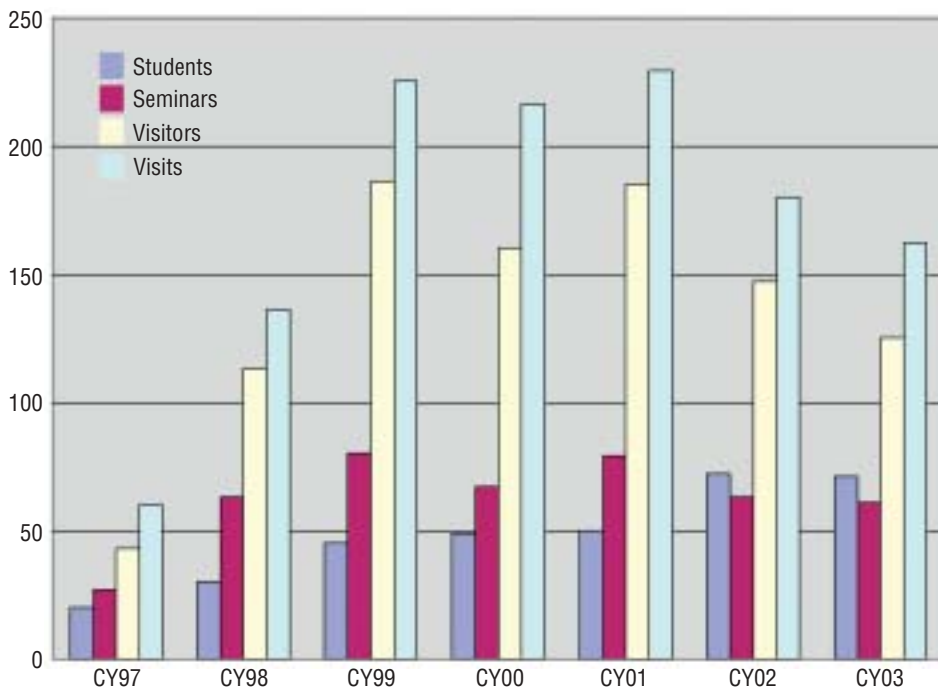


Fig. 1: ISCR Visitor Program CY1997–CY2003

Internships in Terascale Simulation Technology Lecture Series. The tutors included David Brown, Erick Cantu-Paz, Terence Critchlow, Alex Garcia, Jeff Hittinger, Gary Kumfert, Carol Woodward, Kim Yates, CASC's Director Pete Eltgroth, and the ISCR Director. Though the lectures were intended for students, permanent CASC researchers attended an occasional subseries. A reporter from *Science* magazine attended the lecture by Kim Yates on LLNL's future BlueGene/L supercomputer and featured it in a subsequent article.

Recognizing the growing number of computer scientists among the summer students, we added a second track of tutorial lectures during the summer months, called the ISCR Summer Lecture Series. The tutors included computer scientists Gary Kumfert and Kim Yates of CASC, who also

taught in the ITST Lecture Series, as well as Tony Bartoletti, Bill Cabot, Martin Casado, Bronis de Supinski, Paul Dubois, Tina Eliassi-Rad, Chandrika Kamath, Doug Lim, and Valerio Pascucci.

Computer Security specialist Terry Brugger also assembled a summer tutorial lecture series under the ISCR umbrella, under which were included the tutorials of Bartoletti, Cabot, and Casado mentioned above, plus several supplementary topics presented by Brugger, himself.

Figure 1 charts the numbers of visitors and seminars over the past seven years. The number of students in residence in FY'03 remained at its FY'02 high due to the expansion of the ISCR's responsibility in the larger CAR organization. The number of external seminars also remained about the same. (The seminar totals do not include the internally provided tutorial seminars, which doubled from 10 to 20.) The numbers of visits and visitors were slightly down, though the number of visitor-days was at the FY'02 level.

Most of the material of this annual report comes directly from the visitors and principal investigators of the projects being reported. We thank Dean Wheatcraft and Dale Sprouse for their editorial work and Dan Moore of the Technical Information Department of LLNL for his graphic artistry in producing an easily navigated and visually pleasing document.

We hope that you enjoy examining this report on the ISCR's diverse activities in FY 2003. For further information about the Institute, please contact us at the address below. Inquiries about how you might enhance the on-going FY 2004 program at the ISCR, or beyond, are welcome.



David E. Keyes

Institute for Scientific Computing Research
Lawrence Livermore National Laboratory
P. O. Box 808, L-561
Livermore, CA 94551
<http://www.llnl.gov/iscr>



David E. Keyes
Acting Director
<http://www.llnl.gov/iscr/people/keyes>
dekeyes@llnl.gov
925-422-1325



James R. McGraw
Deputy Director
<http://www.llnl.gov/iscr/people/mcgraw>
jmcgraw@llnl.gov
925-422-0541



Linda Becker
Administrator
<http://www.llnl.gov/iscr/people/becker>
becker22@llnl.gov
925-423-0421



Institute for Scientific Computing Research



Institute for Terascale Simulation Lecture Series

(in reverse chronological order)

Institute for Terascale Simulation Lectures

The ASCI Institute for Terascale Simulation Lecture Series was established to enrich the intellectual atmosphere of LLNL's large simulation community through the visits of leaders throughout the diverse areas of computation that undergird simulation. Simulation has become a crucial third mode of scientific investigation and engineering design, along with theory and experiment, and has become especially important for fundamental scientific progress and technical decision support to the U.S. Department of Energy under the Advanced Simulation and Computing Program (ASCI). ITS lectures are designed to appeal to a broad technical audience and are open to all Laboratory staff.

Name, Affiliation, Lecture Date	Page
Hector Garcia-Molina, Stanford University, September 11, 2003	13
Warren Washington, National Center for Atmospheric Research, June 6, 2003.....	14
Stephen Wolfram, Wolfram Research, Inc., April 14, 2003	15

WebBase: Building a Web Warehouse

Hector Garcia-Molina

Stanford University

Email: hector@cs.stanford.edu

Abstract

The World Wide Web, or simply the Web, is rapidly becoming the world's collective information store, containing everything from news to entertainment, personal communications, and product descriptions. This world information store is distributed across millions of computers, but it is often important to gather significant parts of it at a single site. This is one reason to build content indices, such as Google. Another reason is to mine the cached Web, looking for trends or data correlations. A third reason for gathering a Web copy is to create a historical record for Web sites that are ephemeral or changing. In this talk, I will discuss how to build a repository of Web pages, describing some of the technical challenges faced. I will illustrate with some of the work we have been doing in our group at Stanford.

Speaker's web page: <http://www-db.stanford.edu/people/hector.html>

June 6, 2003

Modeling Climate and Future Climate Change

Warren Washington

National Center for Atmospheric Research

Email: wmw@ucar.edu

Abstract

Everyone knows that climate has always changed. So what is unique about what has happened over the last century or so? Many climate research scientists now believe that humans are changing Earth's system and that global warming is taking place. Other scientists are skeptical of this view and think the observed changes result from natural climate variability. A review of recently observed climate change will be presented and compared with climate model simulations of the recent past climate and what is expected in the 21st century. A discussion of the uncertainties will be included along with an analysis of policy options. The future for terascale computing of climate will also be discussed.

Speaker's web page: <http://www.cgd.ucar.edu/ccr/warren/>

A New Kind of Science

Stephen Wolfram

Wolfram Research, Inc.

Email: contact@wolframscience.com

Abstract

Starting from a few computer experiments, Stephen Wolfram has spent more than 20 years developing a new approach to science, described for the first time in his book *A New Kind of Science*. Basic to his approach is the idea of studying not traditional mathematical equations but rules of the kind embodied in the simplest computer programs. A key discovery is that such rules can lead to behavior that shows immense complexity and mirrors many features seen in nature. Wolfram has built on this to tackle a remarkable array of fundamental problems in science, from the origins of apparent randomness in physical systems, to the development of complexity in biology, the ultimate scope and limitations of mathematics, the possibility of a truly fundamental theory of physics, the interplay between free will and determinism, and the character of intelligence in the universe. Released on May 14, 2002, Wolfram's book became an instant bestseller and is now showing many signs of initiating a major paradigm shift in science. Wolfram's presentation will cover some of the key ideas and discoveries in his book, outlining their implications, and discussing their personal and historical context. An extended question and answer period will be included.

Speaker's web page: <http://www.wolframscience.com/events/>



Institute for Scientific Computing Research



Quantum Computation and Information Lecture Series

(in reverse chronological order)

Quantum Computation and Information Seminars

The Quantum Computation and Information Seminar Series was established to provide a perspective and highlights of areas of quantum computation and quantum information useful to LLNL. Held over the course of a year, it featured visiting experts addressing many aspects of quantum information science. This series was co-hosted by the ISCR and the Materials Research Institute at LLNL.

Name, Affiliation, Seminar Date	Page
Stuart Wolf, Univ. of Virginia, May 15, 2003	19
David Meyer, UC San Diego, April 10, 2003	20
Roland Omnès, University Paris-Sud, April 7, 2003	21
Serge Haroche, Collège de France, March 27, 2003	22
Claude Crépeau, McGill University, February 24, 2003	23
Charles Bennett*, IBM T. J. Watson Research Center, February 11, 2003	24
Seth Lloyd, MIT, January 27, 2003	25
Artur Ekert, University of Cambridge, January 21, 2003	26
David Awschalom, UC Santa Barbara, January 10, 2003	27
Sandu Popescu, University of Bristol, December 19, 2002	28
David Wineland, National Institute for Standards and Technology, December 12, 2002	29
Jeff Kimble, California Institute of Technology, December 9, 2002	30
Robert Griffiths, Carnegie-Mellon University, November 4, 2002	31
Anthony J. Leggett*, University of Illinois, Urbana-Champaign, October 22, 2002	32

(*Anthony Leggett and Charles Bennett were part of the QCI Seminar Series but hosted primarily by the LLNL Director through the Director's Distinguished Lecture Series.)

Quantum Information Science and Technology—Defense Advanced Research Projects Agency's (DARPA's) Vision

Stu Wolf

University of Virginia

Abstract

The potential advantages of using quantum mechanical effects in computing and communication have been known for some time. However, up to now, little focused research has addressed the critical issues that would allow the Department of Defense (DoD) communications and/or computational applications to benefit from that potential. QUIST is a comprehensive program designed to address these issues by developing an understanding of the science and theory of quantum information and processing through the demonstration of critical implementations. Specifically, this program will involve the formulation of new algorithms and protocols for ultrasecure (zero probability of intercept) communications. In addition, QUIST will develop and validate new algorithms and methods for solving “quantum complex” problems of importance to DoD—for example, the problem of graph isomorphism, which may have important implications for cryptography and error correction. This program will also explore the limits of quantum computation for dramatically improved speedups of classical computations. Concurrent with these advances, QUIST will develop the component technology for secure quantum communication, including the development of robust megahertz-rate single photon sources and detectors, single quantum bit (qubit) gates, two qubit-controlled NOT gates, and quantum memory. This technology will allow the demonstration of quantum teleportation and ultrasecure communication over long distances (100 km). The development of this technology will provide some of the building blocks for quantum computation, which will require many more quantum gates and larger memory.

April 10, 2003

Algorithms for Quantum Computers

David Meyer

University of California, San Diego

Abstract

Interest in quantum computing exploded after Shor discovered a quantum algorithm to factor numbers exponentially faster than the best classical algorithm known. Despite the importance of this result for the (in)security of classical cryptosystems, other problems with superior quantum solutions must exist to justify the immense commitment of resources that will be necessary to build a quantum computer. In this talk, I will explain Grover's quantum search algorithm and related algorithms with potential applications to problems of interest at Lawrence Livermore National Laboratory, specifically, solving NP problems, simulating classical physical systems, and image processing.

Decoherence and the Problem of Implementing Quantum Computation

Roland Omnès

University Paris-Sud

Abstract

Decoherence is the most troublesome problem in the field of quantum computing. It turns out that the close relation between irreversible phenomena and decoherence yields the current most general theory of decoherence. This relation solves a problem about the existence of a diagonalization basis (pointer basis) of importance for the understanding of decoherence. I will try to make clear the nature of the decoherence, its history, the main problems it raises and their present status, as well as its possible consequences for the prospects of quantum computing.

March 27, 2003

Quantum Information and Decoherence Studies in Cavity QED Experiments

Serge Haroche

Ecole Normale Supérieure and
Collège de France

Abstract

In cavity quantum electrodynamics (QED) experiments, Rydberg atoms and single microwave photons are used as qubits. Quantum gates based on resonant and dispersive atom-field effects have been realized, which implement various kinds of conditional dynamics between these qubits. Three-particle entanglement has been achieved by combining two-qubit operations. A scheme implementing Grover's search algorithms has been proposed. Generalizing these studies to larger systems involving more atoms and photons is challenging. Decoherence produced by field relaxation in the cavity is the most fundamental and difficult effect to control. After a general presentation about our apparatus, we will review these experiments and discuss their possible development, which implies in the short-term improvements in our cavity design and quantitative decoherence studies in the upgraded apparatus. In longer-term projects, we plan to extend our experiments to two cavities and study nonlocal quantum effects involving mesoscopic field superpositions.

Cryptography in the Quantum Computing Era

Claude Crépeau

McGill University

Abstract

Introductions to classical cryptographic tools and quantum computing will first be presented. The basic notion of quantum key distribution will then be discussed. Information on theoretical notions of cryptography over quantum states such as encryption and authentication will be covered. Computational analogues will also be presented: quantum public-key cryptography, public-key authentication, and impossibility of quantum digital signatures. Some applications to quantum error-correcting codes will be presented.

February 11, 2003

Quantum Information

Charles H. Bennett

IBM T. J. Watson Research Center

Abstract

Information and computation theory have recently been extended to include the transmission and processing of intact quantum states and feats such as quantum cryptography, quantum teleportation, and fast quantum computation. Although progress toward a practical quantum computer is slow, the theory of quantum information processing has developed to the point where it can be viewed as the most natural and complete formulation of the notions of information and computation. Quantum information processing extends classical information and computation theory in much the way that complex numbers extend real numbers. In this lecture, we review the capacities of quantum channels and the use of auxiliary resources, such as shared entanglement, in the transmission of classical and quantum information.

So You've Built a Quantum Computer—Now What Are You Going to Do with It?

Seth Lloyd

Massachusetts Institute of
Technology

Abstract

This talk details recent advances in quantum computation and quantum communication. A variety of technologies now exist for constructing simple quantum computers and quantum communication systems. Examples include NMR, quantum optics, and superconducting systems. But once a quantum information processing device has been constructed, what do users do with it? This talk discusses applications of quantum information processing, including quantum algorithms, quantum analog computing, quantum games, quantum internet protocols, and quantum weirdness.

January 21, 2003

Quantum Algorithms: From Quantum Interference to Quantum Annealing

Artur Ekert

University of Cambridge

Abstract

The theory of classical universal computation was laid down in 1936, was implemented within a decade, became commercial within another decade, and dominated the world's economy half a century later. Quantum information technology is a fundamentally new way of harnessing nature. It is too early to say how important this technology will eventually be, but we can reasonably speculate about its effect on computation. Quantum computers use the quantum interference of different computational paths to enhance correct outcomes and suppress erroneous outcomes of computations. A common pattern underpinning quantum algorithms can be identified when quantum computation is viewed as multiparticle interference. I will use this approach to review some of the existing quantum algorithms and to outline new concepts and architectures for implementing quantum computation.

Manipulating Quantum Information with Semiconductor Spintronics

David D. Awschalom

University of California,
Santa Barbara

Abstract

There is a growing interest in the use of electronic and nuclear spins in semiconductor nanostructures as a medium for the manipulation and storage of classical and quantum information. Spin-based electronics offer remarkable opportunities for exploiting the robustness of quantum spin states by combining standard electronics with spin-dependent effects that arise from the interactions between electrons, nuclei, and magnetic fields. In this lecture, we provide an overview of recent developments in coherent electronic spin dynamics in semiconductors and quantum structures, including a discussion of temporally and spatially resolved magnetooptical measurements that reveal an interesting interplay between electronic and nuclear spins. These experiments explore the electronic, photonic, and magnetic control of electron and nuclear spins in a variety of nanostructures and focus on investigating the underlying physics for quantum information processing in the solid state.

December 19, 2002

Quantum Nonlocality

Sandu Popescu
University of Bristol

Abstract

One of the most exotic aspects of the behavior of microscopic particles is the so-called quantum nonlocality, or entanglement. Microscopic particles—or other larger quantum systems—that have interacted in the past and then moved far from each other remain, in a certain sense, connected and can instantaneously “communicate” with each other (in apparent but not real contradiction with Einstein’s relativity). Nonlocality is now considered to be the basic ingredient in the newly developed area of quantum information and computation. In my talk, I will explain at a very accessible level the basic idea of quantum nonlocality, and I will discuss some of its applications.

Quantum Computation with Trapped Atomic Ions

David J. Wineland

National Institute of Standards and
Technology

Abstract

In spite of considerable interest in the possibility of making a quantum computer, it is generally agreed that building one capable of useful factoring or database searching will be extremely difficult. Atomic physics experiments can satisfy many of the requirements for a quantum computer, including a path to realize a large-scale device; however, difficult technical problems must be overcome. Some of these problems, in the context of trapped atomic ions, will be discussed. In the meantime, the ideas of quantum information processing have clarified our thinking about simpler tasks, some of which can now be implemented. For example, simple quantum processing can now increase the signal-to-noise ratio in spectroscopy and may broaden the choices of atoms that can be used for atomic clocks.

December 9, 2002

Quantum Information Science—The Promise, the Problems, and the Plumbing

Jeff H. Kimble

California Institute of Technology

Abstract

In recent years, a remarkable set of advances has occurred at the interface of information science and quantum mechanics, spanning from communication to computation. Quite unexpectedly, certain tasks that are otherwise impossible in the classical world become possible in the quantum realm. This lecture will give an overview of these “quantum miracles,” as well as of the discovery of quantum error correction and fault tolerance that enable reliable computation with imperfect components. A survey of the diverse physical systems that are being explored for the implementation of quantum logic will be presented, with an emphasis on the research at the California Institute of Technology of strong coupling of single atoms and photons, including the realization of quantum teleportation.

The Nature and Location of Quantum Information

Robert B. Griffiths

Carnegie Mellon University

Abstract

Extending the classical information theory of Shannon into the quantum domain runs into the difficulty that textbook quantum theory has no consistent scheme for assigning probabilities to microscopic objects in the absence of measurements. I will discuss how to get around this problem and construct a theory that provides precise answers to questions such as: How many bits of information can be carried by a single qubit? Where is this information located during processes of dense coding and teleportation? Can quantum information travel backward in time? In each case, classical analogies can help us understand the quantum results.

October 22, 2002

Bell's Theorem, Entanglement, Teleportation, Quantum Computing and All That

Anthony Leggett

University of Illinois,
Champaign–Urbana

Abstract

One of the most surprising aspects of quantum mechanics is that under certain circumstances, it does not allow individual physical systems, even when isolated, to possess properties of their own. In the three decades since John Bell first clearly appreciated quantum mechanics revolutionary significance in 1964, this feature has been tested experimentally and spectacularly confirmed, in the opinion of most. More recent discoveries show that it facilitates certain operations that are classically impossible, such as teleportation, secure-in-principle cryptography, and quantum computing (at least in principle). This talk gives a basic introduction to the subject and looks at recent advances that suggest that relatively macroscopic systems (Josephson devices) may be viable candidates for the elements—called qubits—of a quantum computer.